REMARKS

The Examiner has rejected Claims 1, 7, 8, 10-12, 15, 19, 25, 26, 28-30, 33, 37, 43, 44, 46-48, 51, and 55-57 under 35 U.S.C. 103(a) as being unpatentable over Chi (U.S. Patent No. 6,006,329) in view of Farber et al. (U.S. Patent No. 6,415,280) in view of Greschler (U.S. Publication No. 2002/0078203). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims.

With respect to each of the independent claims, the Examiner has relied on the following excerpt from Chi to make a prior art showing of applicant's claimed technique where "audit data generator logic [is]... triggered by said computer virus scanner logic ..." (see this or similar, but not necessarily identical language in the independent claims).

> "When the processor 110 receives a request to scan files for viruses, it sends a request to the storage medium 130 to retrieve the data streams associated with the files that are to be scanned. The retrieved data streams are then written into the system memory 140. The processor 110 then scans the requested data stream in the system memory 140 for viruses." (Chi, Col. 3, lines 17-23 - emphasis added)

Applicant respectfully asserts that the excerpt from Chi relied upon by the Examiner merely teaches what steps are taken "[w]hen the processor 110 receives a request to scan files for viruses" (emphasis added). Specifically, the processor "... sends a request to the storage medium 130 to retrieve the data streams associated with the files that are to be scanned" (emphasis added). However, the processor requesting data streams from the storage medium fails to disclose "audit data generator logic ... triggered by said computer virus scanner logic" (emphasis added), as claimed by applicant.

In addition, with respect to each of the independent claims, the Examiner has relied on the following excerpts from Farber to make a prior art showing of applicant's claimed technique "for identifying a request to execute a computer program and, in response to identification of said request to execute said computer program ..., for

generating audit data identifying said computer program ..." (see this or similar, but not necessarily identical language in the independent claims).

> "A True Name is computed using a function, MD, which reduces a data block B of arbitrary length to a relatively small, fixed size identifier, the True Name of the data block, such that the True Name of the data block is virtually guaranteed to represent the data block B and only data block B." (Farber, Col. 12, lines 38-43 - emphasis added)

> "In operation, data items in the system can be verified and have their integrity checked. This is from the manner in which True Names are determined. This can be used for security purposes, for instance, to check for viruses and to verify that data retrieved from another location is the desired ,and requested data. **For example, the system might store the True Names of all executable applications on the system and then periodically redetermine the True Names of each of these applications to ensure that they match the stored True Names.** Any change in a True Name potentially signals corruption in the system and can be further investigated. The Verify Region background mechanism and the Verify True File extended mechanisms provide direct support for this mode of operation. The Verify Region mechanism is used to ensure that the data items in the True File registry have not been damaged accidentally or maliciously. **The Verify True File mechanism verifies that a data item in a True File registry is indeed the correct data item given its True Name.**" (Farber, Col. 34, lines 45-62 - emphasis added)

Applicant respectfully asserts that the above excerpts from Farber relied upon by the Examiner teach that "the system might store the True Names of all executable applications on the system and then periodically redetermine the True Names of each of these applications to ensure that they match the stored True Names" (emphasis added). Additionally, the excerpts disclose a technique where "[t]he Verify True File mechanism verifies that a data item in a True File registry is indeed the correct data item given its True Name" (emphasis added). However, periodically re-determining and verifying True Names of executable applications simply fails to even suggest a technique "for identifying a request to execute a computer program and, in response to identification of said request to execute said computer program ..., for generating audit data identifying said computer program" (emphasis added), as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, as follows:

> "audit data generator logic separate from said computer virus scanner logic and being triggered by said computer virus scanner logic prior to said generating said scan result, and responsive to said data identifying said computer file to be scanned that is received from said computer virus scanner logic for simultaneously performing additional operations in parallel with said computer virus scan, said additional operations including identifying a request to execute a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner logic and, in response to identification of said request to execute said computer program, generating audit data identifying said computer program" (see this or similar, but not necessarily identical language in each of the independent claims).

Applicant respectfully asserts that the amendments made to the independent claims further distinguish applicant's claimed technique from the prior art references of

Chi and Farber. Specifically, applicant claims that the "audit data generator logic [is] separate from said computer virus scanner logic" (emphasis added). Further, applicant claims that the separate audit data generator logic is "... triggered by said computer virus scanner logic prior to said generating said scan result" (emphasis added). Triggering the separate audit data generator logic allows "for simultaneously performing additional operations in parallel with said computer virus scan" (emphasis added), as claimed by applicant. Additionally, applicant claims that the computer virus scanner "identifyi[es] a request to execute a computer program associated with said computer file to be scanned for computer viruses by said computer virus scanner logic" (emphasis added).

A notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Applicant further notes that the prior art is also deficient with respect to the dependent claims. For example, with respect to Claims 17, 35, and 53, the Examiner has rejected the same under 35 U.S.C. 103(a) as being unpatentable over Chi, in view of Farber, in view of Greschler, in view of Hypponen (U.S. Patent No. 6,577,920). Specifically, the Examiner has relied on the following excerpts from Hypponen to make a prior art showing of applicant's claimed technique "wherein local audit data is stored upon a computer within a computer network until said computer is polled by a remote computer upon said computer network whereupon said local audit data is sent to said remote computer."

> 'Again, a report is sent to the network manager 7, and also possibly to the remote server 17 of the software provider. This report may be accompanied by a copy of the "guilty" macro.' (Hypponen, Col. 5, lines 62-65 - emphasis added)

Applicant respectfully asserts that the excerpt from Hypponen relied upon by the Examiner merely teaches the technique where "a report is sent to the network manager 7, and also possibly to the remote server 17 of the software provider" (emphasis added). However, this prior art reference is deficient since the above excerpt from Hypponen fails to disclose a technique "wherein local audit data is stored upon a computer within a

computer network until said computer is polled by a remote computer" (emphasis added), as claimed by applicant.

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 58-61 below, which are added for full consideration:

"wherein said computer virus scanner logic generates said scan result after receiving a reply from said audit data generator logic" (see Claim 58);

"wherein said computer virus scanner logic generates said scan result as a function of a reply from said audit data generator logic" (see Claim 59);

"wherein a reply from said audit data generator logic is not used by said computer virus scanner logic if said scan result includes a failure" (see Claim 60); and

"wherein said data identifying said computer file is sent to said audit data generator logic prior to performing said computer virus scan" (see Claim 61).

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P456).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100